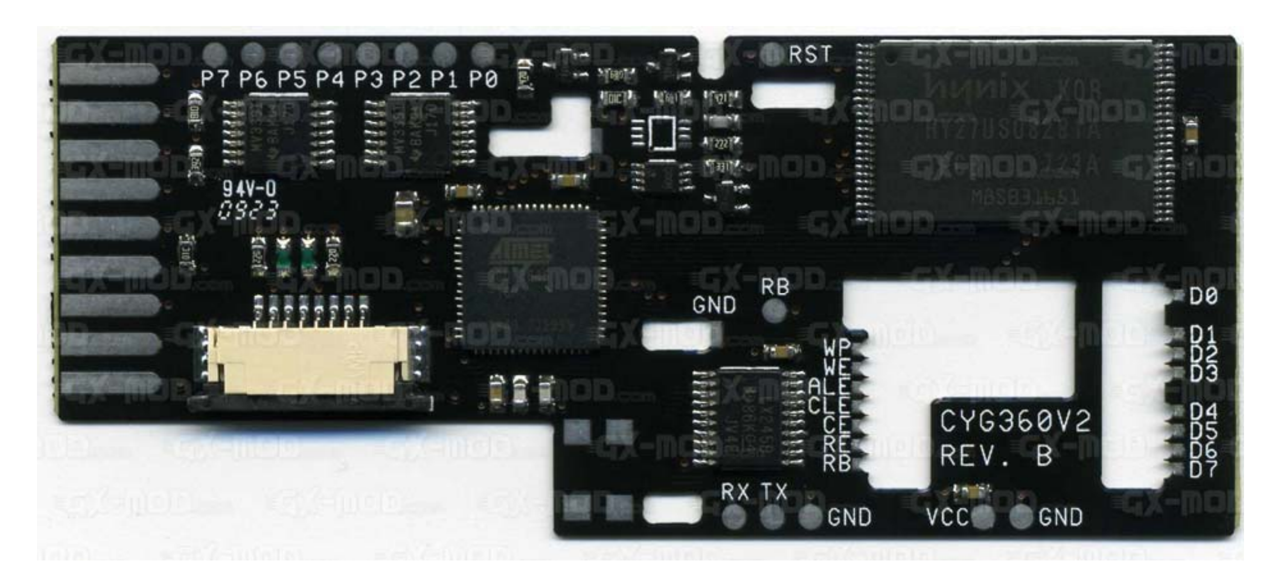
Cygnos360 V2 : intégration du hack JTAG XBox360

La Team Cygnos a publié de nouvelles informations concernant leur puce Cygnos360 v2 qui propose un double-kernel offrant une NAND flash secondaire à votre console. Vous pourrez switcher entre la NAND Flash de votre console et la NAND Flash de la Cygnos360.



Rappel des fonctionnalités :

- Downgrade Xbox360 (production avant Août 2007 et non-HDMI)
- Switch entre le kernel de votre Xbox360 et le kernel de la Cygnos360 V2 (à titre d'exemple pour mettre en place un switch entre une version avec le code région modifié ou un kernel permettant l'utilisation des exploits connus à ce jour)
- Pas besoin de modification du CE-pin ou de couper des pistes
- Protection des données via le stockage des informations sur la NAND Flash de la Cygnos360 V2 et protection contre le ban (Concept dirty-NAND)
- Downgrade direct sur la NAND Flash Cygnos360 V2
- Installation quicksolder de la Cygnos360 V2
- Le firmware de la Cygnos360 V2 peut être modifié à volonté quelque soit la version utilisée
- Utilisation de composants de qualité
- Le downgrade demande environ 1h15m sur un PC moyen. La lecture et l'écriture sur le Flash prend moins d'une minute pour chaque processus
- Utilisation aisée
- Solution avantageuse pour mettre en place un downgrade (version Xenon)
- Lancement de Linux (version Xenon)
- Lecture et écriture de la NAND Xbox 360 en moins d'une minute par processus
- La puce Infectus n'est plus nécessaire pour les fonctions proposées

Les dernières informations communiquées aujourd'hui concernent plusieurs aspects :

- Les soucis de fabrication qui ont retardé le lancement de la puce sont désormais réglés et la production est désormais lancée. Pour le moment la production reste lente mais celle-ci va en s'accélérant et les délais de livraison vont se raccourcir.

- Ce retard a cependant permis d'apporter des améliorations notables au niveau des fonctionnalités et de l'utilisation de la Cygnos360 V2. Les principales nouvelles fonctionnalités concernent :

- L'intégration du hack JTAG dans le firmware de la puce permettant ainsi à celle-ci de jouer le rôle de micro-contrôleur pour l'injection du hack. Cette possibilité est fonctionnelle sur les cartes mères Xenon et Falcon. Les autres révisions devraient suivre via une mise à jour logicielle. Pas de démontage ou de recâblage nécessaire. A noter toutefois qu'il n'est pas (encore) possible de lire et programmer les Jaspers 256 et 512, mais cela est possible sur les Jaspers 16MB.

- La carte USB Cygnos360 V2 possède désormais un connecteur USB vertical. Cela permettra une installation plus propre sur vos Xbox 360.

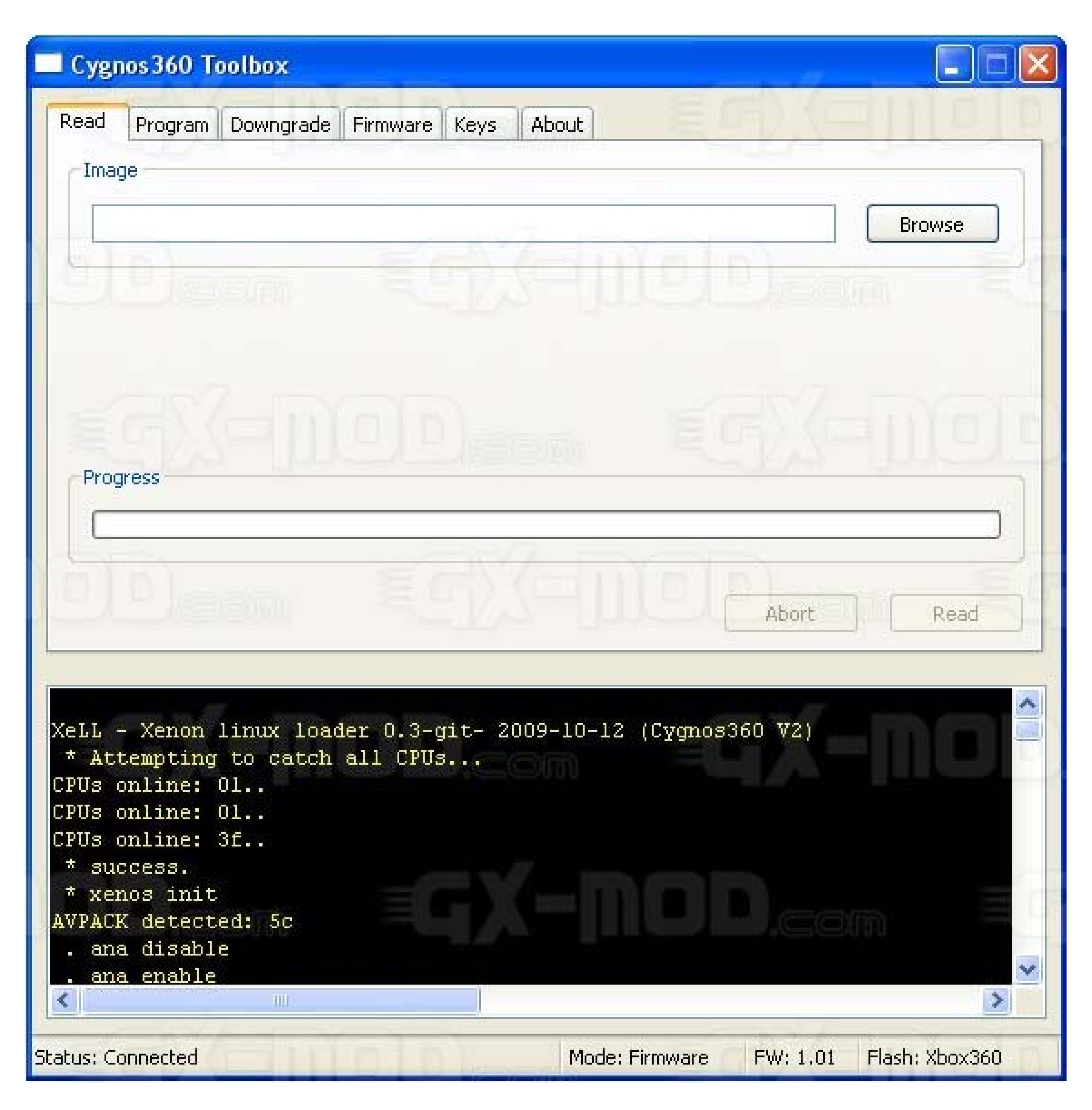


- Ajout de la possibilité de communiquer depuis le "XeLL" vers la Cygnos360 V2, par exemple pour changer de kernel via une commande software (hotswap)

- Ajout d'une fonctionnalité pour activer le changement entre les kernels qui possèdent différentes versions de SMC. Il n'est pas nécessaire de débrancher la console pour effectuer un changement de kernel, ce qui est le case avec les switchers de nand actuel et les solutions XD Card.

- Ajout d'un "canal arrière" sur la Cygnos360 V2 qui permet aux développeur de dialoguer avec les applications fonctionnant sur la Cygnos. De cette façon il est possible par exemple d'envoyer des données depuis la Xbox 360 vers un PC grâce à la Cygnos360 V2 (ex: températures, clés DVD/CPU ou d'autres choses utiles)

- Firmware et Toolbox : Une faille dans le firmware a été corrigée, celle-ci provoquait le fonctionnement du hack JTAG uniquement à chaque mise sous tension. Le hack JTAG a été longuement testé sur Xenon et Falcon. La révision OPUS est très proche de fonctionner aussi bien. Il serait grandement apprécier si des personnes pouvaient tester ceci sur Zephyr.
La nouvelle toolbox en coordination avec le firmware permettra d'afficher des informations depuis le XeLL, Linux, etc dans la partie console de l'application (la partie noire sur la capture d'écran ci-dessous) :



Les parties provenant de la Xbox 360 sont colorées en jaune afin de les distinguer des messages de toolbox (en vert). Du fait que les informations concernant les paramètres fuse proviennent du XeLL, il est désormais très pratique de sauvegarder ces informations dans un fichier. Vous pouvez télécharger le nouveau firmware et toolbox depuis cette page.

- XeLL : Le fait que le micro-contrôleur de la Cygnos ne peut pas gérer les communications issues du port série à 115200 baud, une modification mineure a dû être faite sur XeLL. La modification consiste à paramétrer le registre de la vitesse de transmission de la Xbox 360 à 38400 baud, 8 bits de données, pas de parité et un bit stop. Cela implique que vous devrez

préparer votre propre image du hack JTAG pour la Cygnos360 V2 avec le XeLL modifié Cygnos. Pour se faire vous pouvez télécharger les binaires XeLL et les sources.

- imgbuild : L'outil free60, imgbuild, ne génère pas par défaut une image complète nécessaire à toolbox. Cependant le script a été modifié afin de permettre la correction de ce problème. Vous pouvez télécharger le package complet ici.

La création de votre propre image sous windows nécessite l'installation d'un interpréteur Python. La méthode la plus simple est de télécharger et installer Cygwin puis les packages "python" et "python-crypto" depuis le site Cygwin.

La version modifiée d'imgbuild de la Team Cygnos ne nécessite pas l'ensemble des packages binutils/gcc pour générer une image. Un binaire preload précompilé a été intégré à la place. Le bloc de configuration SMC est, pour sa part, récupéré d'un dump de votre Xbox 360. Une commande typique de génération d'une image devrait ressembler à ceci:

python build.py dump.bin CBxxxx.bin CDxxxx.bin xboxupd.bin smc_hacked.bin xell-1f.bin

CBxxxx.bin et *CDxxxx.bin* sont spécifiques à la console, de même que smc_hacked.bin. Veillez bien à utiliser le xell-1f.bin provenant du package XeLL Cygnos.

- Manuel d'installation : Pour tous ceux que cela intéresse, vous pouvez consulter le manuel d'installation qui contient de nombreuses informations.

Source : GX-Mod